Remarks

In the Office Action dated February 11, 2008, the Examiner rejected claims 17-32 under 35 U.S.C. § 101 as being directed to non-statutory subject matter. The Examiner rejected claims 1, 2, 17 and 18 under 35 U.S.C. § 102 as being anticipated by the article by Batten, et al. "pStore: A Secure Peer-to-Peer Backup System". The Examiner rejected claims 3, 4, 19 and 20 under 35 U.S.C. § 103 as being unpatentable over Batten, et al. in view of Rowstron, et al. "Pastry: Scalable, Decentralized Object Location and Routing for Large-scale Peer-to-peer Systems". The Examiner rejected claims 5-16 and 21-32 under 35 U.S.C. § 103 as being unpatentable over Batten, et al. in view of Elnikety, et al. "Peer-to-Peer Cooperative Backup System".

By this Amendment, Applicants' Attorney has amended claim 23 to change the claim from a method claim to a system claim.

Briefly, the present invention relates to a peer-to-peer method and system for performing and managing backups in a network of nodes which form a cooperative collection of machines having excess storage capacity. A first step in the method includes the step of determining a plurality of peer nodes from the network of nodes for a first node of the network based on the amount of stored data common to both the first node and each of the plurality of peer nodes. The method further includes the step of storing a backup copy of data unique to the first node on each of the plurality of peer nodes so that each of the plurality of peer nodes stores a substantially complete backup of the first node. A system of the present invention performs each of the above-noted method steps.

Clearly, none of the art of record taken either alone or in combination with one another discloses the last claimed feature wherein each of the plurality of peer nodes stores a substantially complete backup of the first node as discussed hereinbelow.

Batten, et al. discloses a variant of a "fine-grained" approach wherein each chunk is stored on nodes with nodeIds numerically closest to the chunk's identifier. Batten, et al. does not exploit inter-host sharing, nor does it address the problem of hosts falsely claiming to store data. As noted in the Abstract of Batten, et al., only 95% of the files in a 13MB dataset can be retrieved when 7 of 30 nodes in a network fail. Obviously, no one peer node, much less a plurality of peer nodes, stores a substantially complete backup of a first node as required by each of the independent claims.

Rowstron, et al. discloses a peer-to-peer network which provides scalable, self-administered routing and node location. The network has a scalable, self-organizing, peer-to-peer routing and object location infrastructure. The network suggests the use of peer-to-peer routing and object storage systems as a substrate for backup.

Elnikety, et al. discloses a cooperative backup scheme that requests random blocks from partners, but assumes that partners either drop all or none of the archived state. Rather than exploit redundancy, Elnikety, et al. use erasure codes to stripe data across several replicas. Such codes allow for low overhead replication, and are tolerant of the failure of one or more replicas. Their main shortcoming is that they require the participation of more than one node for restore.

With respect to the Examiner's rejection under 35 U.S.C. § 101, Applicants' Attorney respectfully disagrees with the Examiner that claims 17-32 can be reasonably interpreted by one of ordinary skill as a system of "software per se". Initially, claims 17-32 require a peer-to-peer system for performing and managing backup in a network of nodes which form a cooperative collection of machines having excess storage capacity. Not only does the system include "means for determining a plurality of peer nodes from the network of nodes for a first node of the network based on an amount of stored data common to both the first node and each of the plurality of nodes", but also the system includes "means for storing a backup copy of data unique to the first node on each of the plurality of peer nodes". Clearly, "software per se" cannot determine a plurality of peer nodes from a network of nodes for a first node of the network and clearly "software per se" cannot store a backup copy of data unique to the first node

on each of the plurality of peer nodes. Rather, an appropriately programmed computer or machine can provide these functions as noted in paragraphs [0045], [0048], [0049], [0064], [0078], [0081], [0082], [0084], [0087], [0093], [0102] and [0108] of corresponding U.S. Published Application No. 2004/0153458.

Clearly, the focus on any analysis under 35 U.S.C. § 101 is whether the claimed system, when viewed as a whole, provides a practical application with a useful result. The entire claim approach establishes that the subject matter of claims 17-32 is patentable in view of 35 U.S.C. § 101. The claimed system for performing and managing backups in a network of nodes clearly provides a practical and useful result as further discussed in the Background Art section of the specification.

Consequently, in view of the above and in the absence of better art, Applicants' Attorney respectfully submits the application is in condition for allowance which allowance is respectfully requested.

Please charge any fees or credit any overpayments as a result of the filing of this paper to our Deposit Account No. 02-3978.

Respectfully submitted,

Brian D. Noble, et al.

By /David R. Syrowik/
    David R. Syrowik
    Reg. No. 27,956
    Attorney/Agent for Applicant

Date: April 8, 2008

BROOKS KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1238
Phone: 248-358-4400
Fax: 248-358-3351